Tampereen yliopisto

Jessica Kuntola

ALKULUKUJEN MÄÄRÄN ÄÄRETTÖMYYS

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Joulukuu 2019

Tiivistelmä

Jessica Kuntola: Alkulukujen määrän äärettömyys
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Joulukuu 2019

Tutkielman tarkoituksena on osoittaa, että alkulukuja on olemassa ääretön määrä. Eukleideen esittämän vanhimman tunnetun todistuksen ja sen muunnelmien lisäksi tutkielmassa esitetään myös sarjan hajaantumista ja Fermat'n lukuja hyödyntävät todistukset alkulukujen äärettömyydestä. Tutkielmassa esitetään myös todistuksia siitä, että muotoa $4n + 3$, $6n + 5$ ja $8n + 3$ olevia alkulukuja on olemassa ääretön määrä.

Näiden todistuksen ymmärtämiseksi tutkielmassa esitetään alkuluvun, suhteellisen alkuluvun, Fermat'n lukujen, neliönjäännöksen ja Legendren symbolin käsitteet. Tutkielmassa on haluttu korostaa sitä, että alkulukujen määrän äärettömyys voidaan todistaa usealla eri tavalla ja sitä, että myös pelkästään tietyissä muodoissa esiintyviä alkulukuja on ääretön määrä.

Avainsanat: lukuteoria, alkuluvut, äärettömyys, Eukleides ja Fermat'n luvut.

Sisältö

1 Johdanto

Tässä tutkielmassa esitetään useita todistuksia alkulukujen määrän äärettömyydestä. Tutkielman ensimmäinen luku käsittelee pohjatietoja, joita hyödynnetään tutkielman aiheen ymmärtämisessä. Pykälässä 2.1 esitetään aiheen ymmärtämiseksi vaadittavien käsitteiden perusmääritelmät sekä niiden havainnollistavat esimerkit.

Pykälässä 2.2 esitetään tutkielman aiheen kannalta tärkeimpien apulauseiden todistukset esimerkkeineen. Pykälä 2.3 johdattelee pääaiheeseen käsittelemällä lyhyesti sitä, miten alkulukuja voidaan yleisesti määrittää.

Toinen luku käsittelee todistuksia alkulukujen määrän äärettömyydestä. Luvun ensimmäisessä pykälässä 3.1 esitetään Eukleideen antama vanhin tunnettu todistus aiheesta sekä siitä tehtyjä muunnelmia. Pykälässä 3.2 esitetään sarjan hajaantumista hyödyntävä todistus ja pykälässä 3.3 Fermat'n lukuja ja niiden ominaisuuksia hyödyntävä todistus alkulukujen äärettömyydestä.

Pykälässä 3.4 todistetaan muotoa $4n+3$ ja $6n+5$ olevien alkulukujen äärettömyys. Viimeisessä pykälässä 3.5 todistetaan neliönjäännöstä ja Legendren symbolia sekä niiden ominaisuuksia hyödyntäen muotoa $8n+3$ olevien alkulukujen äärettömyys.

Tutkielman sisällön ymmärtämiseen vaadittavat tärkeimmät käsitteet on määritelty, mutta lukijan oletetaan hallitsevan lukuteorian ja algebran perusteita kuten jaollisuuden ja kongruenssin ominaisuudet.

Päälähdeteoksena tutkielmassa käytetään Finen ja Rosenbergerin kirjaa Number theory: An introduction via the distribution of primes. Tämän lisäksi lähdeteoksina on käytetty myös Burtonin kirjaa Elementary number theory ja Rosenin kirjaa Elementary number theory and its applications.

2 Alkuluvut

2.1 Perusmääritelmiä

Luvussa 2 käsitellään alkulukujen äärettömyyden ymmärtämiseen vaadittavia pohjatietoja. Tässä pykälässä 2.1 esitetään aiheeseen liittyviä perusmääritelmiä sekä niitä havainnollistavia esimerkkejä.

Määritelmä 2.1. (Vrt. [3, s. 70].) Olkoon p lukua 1 suurempi positiivinen kokonaisluku. Lukua p kutsutaan *alkuluvuksi*, mikäli sen ainoat positiiviset jakajat ovat 1 ja p.

Esimerkki 2.2. Kokonaisluvut 2, 3, 5, 17, 29, 61, 101 ja 157 ovat alkulukuja.

Määritelmä 2.3. (Vrt. [3, s. 70].) Lukua 1 suurempaa positiivista kokonaislukua, joka ei ole alkuluku, kutsutaan *yhdistetyksi luvuksi*.

Esimerkki 2.4. Kokonaisluvut $4 = 2 \cdot 2$, $33 = 3 \cdot 11$, $153 = 3 \cdot 51$ ja $178 = 2 \cdot 89$ ovat yhdistettyjä lukuja.

Määritelmä 2.5. (Vrt. [3, s. 39].) Kokonaislukujen $a \neq 0$ ja $b \neq 0$ *suurin yhteinen tekijä* on suurin kokonaisluku n, joka jakaa sekä luvun a että luvun b. Sitä merkitään notaatiolla $\text{syt}(a, b) = n$.

Esimerkki 2.6. Olkoon $a = 15$ ja $b = 24$. Nyt koska $15 = 3 \cdot 5$ ja $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$, niin määritelmän 2.5 perusteella $\text{syt}(15, 24) = 3$.

Määritelmä 2.7. (Vrt. [3, s. 39].) Kokonaislukuja a ja b, missä $a \neq 0$ tai $b \neq 0$, kutsutaan *suhteellisiksi alkuluvuiksi*, jos $\text{syt}(a, b) = 1$.

Esimerkki 2.8. Koska $\text{syt}(12, 13) = 1$, niin 12 ja 13 ovat suhteellisia alkulukuja.

2.2 Avustavia lauseita

Tässä pykälässä 2.2 esitetään alkulukujen äärettömyyden todistamisen yhteydessä tarvittava aritmetiikan peruslause 2.17 sekä sen todistamiseen vaadittavat apulauseet.

Seuraavaa apulausetta 2.9 kutsutaan yleisesti *Eukleideen lemman* yleistykseksi.

Apulause 2.9. Oletetaan, että $a \mid bc$ ja $\text{syt}(a, b) = 1$. Tällöin $a \mid c$.

Todistus. (Vrt. [2, s. 15].) Oletetaan, että $\text{syt}(a, b) = 1$. Tällöin 1 voidaan ilmaista lukujen a ja b lineaarikombinaationa (ks. [1, s. 23]) siten, että

$$ax + by = 1.$$

Kertomalla lausekkeen molemmat puolet luvulla c saadaan

$$(ax + by)c = axc + byc = c.$$

Koska $a \mid a$ ja $a \mid bc$, niin $a \mid (axc + byc)$. Tästä seuraa, että $a \mid c$. □

Esimerkki 2.10. Olkoon $a = 5$, $b = 7$ ja $c = 10$. Nyt $\text{syt}(5, 7) = 1$ ja $5 \mid 70 = 7 \cdot 10$, joten $5 \mid 70$.

Seuraavaa apulausetta 2.11 kutsutaan myös *Eukleideen lemmaksi*, mutta edellisestä poiketen apulause koskee alkulukuja kaikkien kokonaislukujen sijaan. Apulauseelle esitetään myös kaksi seurausta, joista jälkimmäistä 2.15 hyödynnetään *aritmetiikan peruslauseen* 2.17 todistamisessa.

Apulause 2.11. Jos p on alkuluku, $a, b \in \mathbb{Z}^+$ ja $p \mid ab$, niin $p \mid a$ tai $p \mid b$.

Todistus. (Vrt. [2, s. 17].) Oletetaan, että $p \mid ab$. Nyt jos a ei ole jaollinen luvulla p, niin a ja p ovat suhteellisia alkulukuja siten, että $\text{syt}(a, p) = 1$. Tällöin apulauseen 2.9 perusteella $p \mid b$. □

Esimerkki 2.12. Tiedetään, että 5 on alkuluku, $5 \mid 40$ ja $40 = 4 \cdot 10$. Tällöin $5 \mid 4 \cdot 10$ ja $5 \mid 10$, joten 5 jakaa ainakin toisen tulon tekijöistä.

Seuraus 2.13. *Jos p on alkuluku ja $p \mid a_1 a_2 \cdots a_n$, niin $p \mid a_k$ jollakin indeksin k arvolla, missä $1 \leq k \leq n$.*

Todistus. Ks. [1, s. 40]. □

Esimerkki 2.14. Tiedetään, että 7 on alkuluku, $7 \mid 70$ ja $70 = 7 \cdot 10$. Nyt myös $7 \mid 7$, joten 7 jakaa ainakin yhden tulon tekijöistä.

Seuraus 2.15. *Jos $p, q_1, q_2, \ldots, q_n$ ovat kaikki alkulukuja ja $p \mid q_1 q_2 \cdots q_n$, niin $p = q_k$ jollakin indeksin k arvolla, missä $1 \leq k \leq n$.*

Todistus. (Vrt. [1, s. 40].) Seurauksen 2.13 nojalla tiedetään, että $p \mid q_k$ jollakin indeksin k arvolla, kun $1 \leq k \leq n$. Nyt koska q_k on alkuluku, niin sen ainoat positiiviset kokonaislukujakajat ovat 1 ja q_k. Edelleen koska $p > 1$, niin täytyy olla, että $p = q_k$. □

Esimerkki 2.16. Tiedetään, että 5 on alkuluku, $5 \mid 50$ ja $50 = 5 \cdot 5 \cdot 2$. Nyt myös $5 \mid 5$, joten 5 on yksi alkuluvuista koostuvan tulon tekijöistä.

Seuraavaa apulausetta 2.17 kutsutaan yleisesti *aritmetiikan peruslauseeksi*. Lauseen todistamisessa on käytetty apuna hyvänjärjestyksenperiaatetta sekä edellä esitettyjä apulauseita ja seurausta 2.15.

Hyvänjärjestyksenperiaate. (Vrt. [1, s. 1].) Jokainen ei-negatiivisia kokonaislukuja sisältävä epätyhjä joukko S sisältää aina pienimmän alkion. Tällöin on olemassa joukkoon S kuuluva kokonaisluku a siten, että $a \leq b$ aina, kun $b \in S$.

Apulause 2.17. Jokainen kokonaisluku $n \geq 2$ voidaan esittää alkulukujen tulona. Saatu tulo on tekijöiden järjestystä vaille yksikäsitteinen.

Todistus. (Vrt. [1, ss. 41–42].) Valitaan mielivaltainen kokonaisluku n, joka on joko alkuluku tai yhdistetty luku. Jos n on alkuluku, niin lause on todistettu. Olkoon n siis yhdistetty luku. Nyt on olemassa kokonaisluku d siten, että $d \mid n$ ja $1 < d < n$. Hyvänjärjestyksenperiaatteen mukaisesti valitaan kaikkien mahdollisten kokonaislukujen d joukosta pienin, jota merkitään symbolilla p_1. Nyt luvun p_1 on oltava alkuluku. Muutoin myös sillä olisi jakaja q, missä $1 < q < p_1$. Tällöin $q \mid p_1$ ja $p_1 \mid n$, mistä seuraisi $q \mid n$. Tämä on ristiriidassa sen kanssa, että p_1 olisi luvun n pienin jakaja, kun $p_1 > 1$.

Tämän perusteella voidaan kirjoittaa $n = p_1 n_1$, missä p_1 on alkuluku ja $1 < n_1 < n$. Nyt jos n_1 on alkuluku, niin lause on todistettu. Jos n_1 ei ole alkuluku, niin voidaan edellä käytetyllä tavalla valita toinen alkuluku p_2 siten, että $n_1 = p_2 n_2$. Tällöin

$$n = p_1 p_2 n_2 \qquad (1 < n_2 < n_1).$$

Nyt jos n_2 on alkuluku, niin lause on todistettu. Jos n_2 ei ole alkuluku, niin voidaan kirjoittaa $n_2 = p_3 n_3$, missä p_3 on alkuluku. Tällöin

$$n = p_1 p_2 p_3 n_3 \qquad (1 < n_3 < n_2).$$

Vähenevä jono

$$n > n_1 > n_2 > \cdots > 1$$

ei voi jatkua äärettömästi, joten äärellisen välivaiheiden määrän jälkeen n_{k-1} on alkuluku, jota merkitään symbolilla p_k. Tämä johtaa alkutekijähajotelmaan

$$n = p_1 p_2 \cdots p_k.$$

Todistetaan vielä, että alkutekijähajotelma on yksikäsitteinen. Oletetaan, että kokonaisluku n voidaan esittää alkulukujen tulona kahdella eri tavalla

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad (r \leq s),$$

missä p_i ja q_j ovat kaikki suuruusjärjestykseen kirjoitettuja alkulukuja siten, että

$$p_1 \leq p_2 \leq \cdots \leq p_r \quad \text{ja} \quad q_1 \leq q_2 \leq \cdots \leq q_s.$$

Koska $p_1 \mid q_1 q_2 \ldots q_s$, niin apulauseen 2.11 seurauksen 2.15 perusteella $p_1 = q_k$ jollakin indeksin k arvolla. Tästä seuraa, että $p_1 \geq q_1$. Vastaavasti $q_1 \geq p_1$, mistä seuraa, että $p_1 = q_1$. Supistamalla tämä yhteinen tekijä saadaan

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

Toistamalla edellinen vaihe saadaan $p_2 = q_2$, jolloin

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s.$$

Jatketaan vastaavasti. Jos epäyhtälö $r < s$ säilyisi, päädyttäisiin lopulta tilanteeseen

$$1 = q_{r+1} q_{r+2} \cdots q_s,$$

mikä ei ole mahdollinen, koska jokainen $q_j > 1$. Tällöin $r = s$ ja

$$p_1 = q_1, \quad p_2 = q_2, \ \ldots, \quad p_r = q_r,$$

jolloin luvun n kaksi alkutekijähajotelmaa ovat samat. Tällöin alkutekijähajotelma on yksikäsitteinen. □

Esimerkki 2.18. Kokonaisluku 220 voidaan kirjoittaa muodossa $220 = 2 \cdot 2 \cdot 5 \cdot 11 = 2^2 \cdot 5 \cdot 11$.

2.3 Alkulukujen määrittäminen

Tässä pykälässä 2.3 esitetään yleinen alkulukutesti ja taulukointia hyödyntävä Eratostheneen seula, joiden avulla voidaan määrittää lukua n pienempiä alkulukuja.

Yleinen alkulukutesti. (Vrt. [2, s. 198].) Olkoon p alkuluku ja $n > 0$ siten, että $p \leq \sqrt{n}$. Kokonaisluku n on alkuluku, jos ja vain jos se ei ole jaollinen millään tällaisella alkuluvulla p.

Esimerkki 2.19. Tarkastellaan kokonaislukua 127. Nyt $11 < \sqrt{127} < 12$. Tällöin on testattava, onko 127 jaollinen jollain luvuista 2, 3, 5, 7 tai 11. Mikään näistä luvuista ei jaa lukua 127, joten se on alkulukutestin perusteella alkuluku.

Eratostheneen seula. (Vrt. [2, s. 199].) Valitaan jokin $n > 0$. Taulukoidaan nyt kaikki ne positiiviset kokonaisluvut $x_1, x_2, \ldots, x_p$, jotka ovat pienempiä tai yhtä suuria kuin n. Valitaan sitten pienin alkuluku 2 ja eliminoidaan taulukosta kaikki ne kokonaisluvut, jotka ovat jaollisia luvulla 2. Seuraavaksi eliminoidaan ne kokonaisluvut, joita ei ole vielä eliminoitu ja jotka ovat jaollisia luvulla 3. Seuraavan eliminoimattoman kokonaisluvun 5 kohdalla toimitaan vastaavasti. Jatketaan luvun $\sqrt{n}$ kokonaisosaan saakka. Tällöin jäljelle jääneet luvut ovat alkulukuja.

Esimerkki 2.20. Tarkastellaan kokonaislukua 64. Siitä voidaan muodostaa seuraavanlainen taulukko:

	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Nyt koska $\sqrt{64} = 8$, niin eliminoidaan taulukosta lukujen n monikerrat, kun $n \leq 8$, jolloin saadaan seuraavanlainen taulukko:

	2	3		5		7	
		11		13			
17		19				23	
				29		31	
				37			
41		43				47	
				53			
		59		61			

Näin ollen *Eratostheneen seulan* mukaisesti kokonaislukua 64 pienemmät alkuluvut ovat 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 ja 61.

3 Alkulukujen määrän äärettömyys

3.1 Eukleideen todistus

Pykälässä 2.3 esitettiin, miten alkulukuja voidaan määrittää. Alkulukujen määrittäminen esitetyillä keinoilla on kuitenkin mahdollista vain tiettyyn rajaan saakka. Luvussa 3 esitetäänkin useita todistuksia siitä, että alkulukuja on olemassa ääretön määrä.

Ensimmäiseksi esitetään kreikkalaisen matemaatikon Eukleideen antama vanhin tunnettu todistus alkulukujen äärettömyydelle. Todistuksessa hyödynnetään pykälässä 2.2 esitettyjä apulauseita.

Lause 3.1. *Alkulukuja on ääretön määrä.*

Todistus. (Vrt. [2, s. 17].) Tehdään vastaoletus, että alkulukuja on äärellinen määrä. Merkitään niitä symboleilla $p_1, \ldots, p_n$. Jokainen alkuluku on positiivinen, joten voidaan muodostaa positiivinen kokonaisluku

$$N = p_1 p_2 \cdots p_n + 1.$$

Lauseen 2.17 perusteella N voidaan esittää alkulukujen tulona. Tällöin on olemassa alkuluku p, joka jakaa kokonaisluvun N eli

$$p \mid p_1 p_2 \cdots p_n + 1.$$

Ainoat oletetut alkuluvut ovat $p_1, p_2, \ldots, p_n$, joten siitä seuraa, että $p = p_i$ jollakin indeksin i arvolla, missä $i = 1, \ldots, n$. Tiedetään myös, että $p \mid p_1 p_2 \cdots p_i \cdots p_n$. Nyt p ei voi jakaa lukua $p_1 p_2 \cdots p_n + 1$, koska $p_i \nmid 1$, sillä pienin mahdollinen alkuluku on 2. Kyseessä on siis ristiriita. Tällöin p ei kuulu oletettujen alkulukujen joukkoon, mikä tarkoittaa, että alkulukuja on oltava ääretön määrä. □

Seuraavaksi esitetään kaksi vaihtoehtoista todistusta lauseelle 3.1. Ensimmäisessä hyödynnetään osajoukkoihin jakamista ja toisessa kertomia.

Todistus. (Vrt. [2, s. 56].) Tehdään vastaoletus, että alkulukuja on vain äärellinen määrä $p_1, \ldots, p_n$, missä $n \geq 2$. Olkoon $P = \{ p_1, \ldots, p_n \}$. Jaetaan P kahteen erilliseen epätyhjään osajoukkoon P_1 ja P_2.

Tarkastellaan nyt lukua $m = q_1 + q_2$, missä q_1 on osajoukon P_1 ja q_2 osajoukon P_2 alkulukujen tulo. Olkoon p alkuluku, joka jakaa luvun m. Koska $p \in P$, niin siitä seuraa, että p jakaa toisen luvuista q_1 ja q_2. Koska p ei jaa molempia lukuja, niin se ei jaa lukua m, mikä on ristiriita. Tällöin p ei ole yksi oletuista alkuluvuista, jolloin alkulukujen lukumäärän on oltava ääretön. □

Todistus. (Vrt. [2, s. 56].) Tehdään vastaoletus, että alkulukuja on vain äärellinen määrä $p_1, \ldots, p_n$ ja olkoon $N = p_1 \cdots p_n$. Lisäksi $p_i < N$ jokaisella indeksin i arvolla. Olkoon q pienin alkuluku, joka jakaa luvun $N! + 1$.

Nyt jos $q < N$, niin q jakaa luvun $N!$, joten se ei voi jakaa lukua $N! + 1$. Tämän vuoksi on oltava $q > N$, jonka seurauksena $q > p_i$, kun $i = 1, \ldots, n$. Tällöin $q \neq p_i$, kun $i = 1, \ldots, n$, mikä on ristiriita. Tällöin alkulukujen lukujono on ääretön. □

3.2 Äärettömyys sarjan hajaantumisen avulla

Luvussa 3.2 esitetään sarjan hajaantumista hyödyntävä todistus 3.3 alkulukujen äärettömyydelle. Sen todistamisessa hyödynnettään apulausetta 3.2.

Apulause 3.2. Jos $p_1, \ldots, p_k, \ldots$ on alkulukujen jono kasvavassa järjestyksessä, niin $p_n \leq 2^{2^{n-1}}$ kaikilla indeksin n arvoilla ja $p_n < 2^{2^{n-1}}$ kaikilla indeksin n arvoilla, kun $n > 1$.

Todistus. Ks. [2, s. 58]. □

Lause 3.3. *Sarja $\sum_{p=alkuluku} \frac{1}{p}$ hajaantuu. Tällöin erityisesti alkulukujen lukujono on ääretön.*

Todistus. (Vrt. [2, ss. 58–59].) Jos sarja $\sum_{p=alkuluku} \frac{1}{p}$ hajaantuu, niin on olemassa ääretön määrä alkulukuja. Muussa tapauksessa kyseessä olisi äärellinen sarja.

Olkoon $p_1, \ldots, p_k, \ldots$ alkulukujen lukujono kasvavassa järjestyksessä. Kyseessä voi olla äärellinen tai ääretön lukujono. Nyt apulauseen 3.2 perusteella $p_n \leq 2^{2^{n-1}}$ kaikilla indeksin n arvoilla ja $p_n < 2^{2^{n-1}}$ kaikilla indeksin n arvoilla, kun $n > 1$.

Oletetaan, että

$$\sum_{\text{p = alkuluku}} \frac{1}{p} = \sum_{i=1}^{\infty} \frac{1}{p_i}$$

suppenee. Alkulukujen äärellisyyttä ei oleteta eli, jos alkulukuja on äärellinen määrä, on kyseessä äärellinen summa. Koska sarja suppenee ja lukujono p_i kasvaa, niin on

olemassa N siten, että

$$\sum_{i=N+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}. \tag{3.1}$$

Kiinnitetään N. Olkoon $Q_N(x)$ niiden positiivisten kokonaislukujen lukumäärä, jotka ovat pienempiä tai yhtä suuria kuin luonnollinen luku x ja jotka eivät ole jaollisia millään alkuluvuista $p_{N+1}, p_{N+2}, \ldots$. Nyt niiden kokonaislukujen lukumäärä, joille pätee, että $n \leq x$ ja jotka ovat jaollisia jollakin oletuksen mukaisella alkuluvulla p, on pienempi kuin $\frac{x}{p}$. Sen seurauksena jokaiselle kokonaisluvulle x pätee oletuksen 3.1 perusteella

$$x - Q_N(x) < \frac{x}{p_{N+1}} + \frac{x}{p_{N+2}} + \cdots < \frac{x}{2}.$$

Tällöin $\frac{x}{2} < Q_N(x)$. Toisaalta, jos $n < x$ ja n ei ole jaollinen millään luvuista $p_{N+1}, p_{N+2}, \ldots$, niin $n = n_1^2 m$, missä m on neliötön. Sen seurauksena $m = 2^{e_1} 3^{e_2} \cdots p_N^{e_N}$, missä jokainen $e_i = 0$ tai $e_i = 1$. Tällöin on olemassa enintään 2^N vaihtoehtoa luvulle m. Lisäksi on olemassa enintään $\sqrt{x}$ vaihtoehtoa luvulle n_1. Tästä seuraa, että

$$\frac{x}{2} < Q_N(x) < 2^N \sqrt{x}.$$

Koska N on kiinnitetty, on kyseessä ristiriita, kun x on riittävän suuri. Tällöin $\sum_{p=alkuluku} \frac{1}{p}$ hajaantuu, joten alkulukuja on olemassa ääretön määrä. □

3.3 Äärettömyys Fermat'n lukujen perusteella

Pykälässä 3.3 esitetään Fermat'n lukuja hyödyntävä todistus 3.13 alkulukujen äärettömyydestä. Todistuksessa käytetään apuna lausetta 3.11, jossa osoitetaan, että kaksi toisistaan eroavaa Fermat'n lukua ovat suhteellisia alkulukuja. Tämän todistamisessa auttaa kokonaislukujen jaollisuutta käsittelevä lause 3.7 sekä apulause 3.9.

Aloitetaan määrittelemällä Fermat'n luvut.

Määritelmä 3.4. (Vrt. [3, s. 132].) Muotoa $F_n = 2^{2^n} + 1$ olevia kokonaislukuja kutsutaan *Fermat'n luvuiksi*.

Esimerkki 3.5. Kokonaisluku 257 voidaan esittää muodossa $257 = 2^8 + 1 = 2^{2 \cdot 2^2} + 1 = 2^{2^3} + 1$. Tällöin määritelmän 3.4 nojalla 257 on Fermat'n luku.

Esimerkki 3.6. Kokonaisluku 30 ei ole Fermat'n luku, sillä $30 = 2 \cdot 3 \cdot 5$, joten sitä ei voi esittää muodossa $2^{2^n} + 1$.

Lause 3.7. *Jos a, b ja c ovat kokonaislukuja siten, että $a \mid b$ ja $b \mid c$, niin $a \mid c$.*

Todistus. (Vrt. [3, s. 37].) Oletetaan, että $a \mid b$ ja $b \mid c$. Nyt on olemassa kokonaisluvut d ja e siten, että $ad = b$ ja $be = c$. Tällöin $c = be = (ad)e = a(de)$, joten $a \mid c$. □

Esimerkki 3.8. Olkoon $a = 3$, $b = 9$ ja $c = 18$. Nyt koska $3 \mid 9$ ja $9 \mid 18$, niin lauseen 3.7 perusteella $3 \mid 18$.

Apulause 3.9. Olkoon $F_k = 2^{2^k} + 1$ k. Fermat'n luku, missä $k \geq 0$. Nyt kaikille positiivisille kokonaisluvuille n pätee, että

$$F_0 F_1 F_2 \cdots F_{n-1} = F_n - 2.$$

Todistus. (Vrt. [3, ss. 133–134].) Todistetaan induktiolla luvun n suhteen.

Perusaskeleessa voidaan todeta, että kun $n = 1$, niin

$$F_0 = F_1 - 2,$$

joten lause pätee, sillä $F_0 = 3$ ja $F_1 = 5$. Tehdään sitten induktio-oletus, että lause pätee positiiviselle kokonaisluvulle n siten, että

$$F_0 F_1 F_2 \cdots F_{n-1} = F_n - 2.$$

Induktio-oletuksen perusteella voidaan todistaa induktioväite, että lause pätee kokonaisluvulle $n + 1$, sillä

$$\begin{aligned} F_0 F_1 F_2 \cdots F_{n-1} F_n &= (F_0 F_1 F_2 \cdots F_{n-1}) F_n \\ &= (F_n - 2) F_n = (2^{2^n} - 1)(2^{2^n} + 1) \\ &= (2^{2^n})^2 - 1 = 2^{2^{n+1}} - 1 = F_{n+1} - 2. \end{aligned}$$

Induktioperiaatteen nojalla lause pitää paikkansa. □

Esimerkki 3.10. Olkoon $n = 5$. Nyt apulauseen 3.9 mukaisesti

$$\begin{aligned} F_0 F_1 F_2 F_3 F_4 &= (2^{2^0} + 1)(2^{2^1} + 1)(2^{2^2} + 1)(2^{2^3} + 1)(2^{2^4} + 1) \\ &= 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65\,537 = (2^{2^5} + 1) - 2 = F_5 - 2. \end{aligned}$$

Lause 3.11. *Olkoot m ja n toisistaan eroavia kokonaislukuja siten, että $m \geq 0$ ja $n \geq 0$. Tällöin Fermat'n luvut F_m ja F_n ovat suhteellisia alkulukuja.*

Todistus. (Vrt. [3, s. 134].) Oletetaan, että $m < n$. Nyt apulauseen 3.9 nojalla tiedetään, että

$$F_0F_1F_2 \cdots F_m \cdots F_{n-1} = F_n - 2.$$

Oletetaan nyt, että luvuilla F_m ja F_n on yhteinen jakaja d. Tällöin tiedetään lauseen 3.7 perusteella, että

$$d \mid (F_n - F_0F_1F_2 \cdots F_m \cdots F_{n-1}) = 2.$$

Tällöin joko $d = 1$ tai $d = 2$. Nyt Fermat'n lukujen määritelmän 3.4 perusteella tiedetään, että Fermat'n luvut ovat parittomia, joten on oltava, että $d = 1$. Tällöin $\text{syt}(F_m, F_n) = 1$, joten F_m ja F_n ovat suhteellisia alkulukuja. □

Esimerkki 3.12. Olkoon $m = 3$ ja $n = 4$. Tällöin $F_m = 2^{2^3} + 1 = 257$ ja $F_n = 2^{2^4} + 1 = 65\,537$. Nyt sekä F_n että F_m ovat alkulukuja, joten $\text{syt}(257, 65\,537) = 1$. Tämä tarkoittaa, että F_n ja F_m ovat suhteellisia alkulukuja.

Lause 3.13. *Alkulukuja on ääretön määrä.*

Todistus. (Vrt. [3, s. 134].) Aritmetiikan peruslauseen 2.17 perusteella jokaisella Fermat'n luvulla F_n on alkulukujakaja p_n. Nyt koska $\text{syt}(F_m, F_n) = 1$, niin tiedetään, että $p_m \neq p_n$ aina, kun $m \neq n$. Näin ollen on alkulukuja oltava ääretön määrä. □

3.4 Muotoa $4n + 3$ ja $6n + 5$ olevat alkuluvut

Pykälissä 3.4 ja 3.5 osoitetaan, että tiettyä muotoa olevia alkulukuja on olemassa ääretön määrä. Tässä pykälässä käsitellään muotoa $4n+3$ ja $6n+5$ olevia alkulukuja.

Esitetään ensin todistus 3.16 muotoa $4n+3$ olevien alkulukujen äärettömyydelle. Todistuksen apuna on käytetty apulausetta 3.14.

Apulause 3.14. Kahden tai useamman muotoa $4n + 1$ olevan kokonaisluvun tulo on edelleen muotoa $4n + 1$.

Todistus. (Vrt. [1, s. 53].) Todistuksessa riittää tarkastella kahden kokonaisluvun tuloa. Olkoon $k = 4n + 1$ ja $k' = 4m + 1$. Kertomalla nämä luvut yhteen saadaan

$$kk' = (4n + 1)(4m + 1) = 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1,$$

mikä on muotoa $4n + 1$, joten apulause pitää paikkansa. □

Esimerkki 3.15. Olkoon $n_1 = 2$, $n_2 = 3$ ja $n_3 = 5$. Nyt

$$\begin{aligned}(4n_1+1)(4n_2+1)(4n_3+1) &= (4\cdot 2+1)(4\cdot 3+1)(4\cdot 5+1) = (8+1)(12+1)(20+1)\\ &= 9\cdot 13\cdot 21 = 2457 = 2456+1 = 4\cdot 614+1.\end{aligned}$$

Kolmen muotoa $4n+1$ olevan kokonaisluvun tulo on muotoa $4n+1$.

Lause 3.16. *On olemassa ääretön määrä alkulukuja, jotka ovat muotoa $4n+3$.*

Todistus. (Vrt. [1, s. 54]). Tehdään vastaoletus, että on olemassa äärellinen määrä muotoa $4n+3$ olevia alkulukuja. Merkitään niitä symboleilla $q_1, q_2, \ldots, q_s$. Tarkastellaan positiivista kokonaislukua

$$N = 4q_1q_2\cdots q_s - 1 = 4(q_1q_2\cdots q_s - 1) + 3,$$

ja olkoon $N = r_1r_2\cdots r_t$ sen alkutekijähajotelma (ks. apulause 2.17). Koska N on pariton kokonaisluku, niin $r_k \neq 2$ pätee kaikilla indeksin k arvoilla, joten r_k on joko muotoa $4n+1$ tai muotoa $4n+3$. Apulauseen 3.14 perusteella muotoa $4n+1$ olevien alkulukujen tulo on muotoa $4n+1$. Nyt N on selvästi muotoa $4n+3$, joten se sisältää ainakin yhden alkulukutekijän r_i, joka on muotoa $4n+3$. Nyt r_i ei kuitenkaan voi olla mikään alkuluvuista $q_1, q_2, \ldots, q_s$, koska muutoin $r_i \mid 1$, mikä ei ole mahdollista, koska pienin mahdollinen alkuluku on 2. Kyseessä on siis ristiriita, mistä seuraa, että on olemassa ääretön määrä muotoa $4n+3$ olevia alkulukuja. □

Esitetään vielä toinen samankaltainen todistus (ks. lause 3.19) muotoa $6n+5$ olevien alkulukujen äärettömyydelle. Todistuksessa on käytetty apuna apulausetta 3.17.

Apulause 3.17. Kahden tai useamman muotoa $6n+1$ olevan kokonaisluvun tulo on edelleen muotoa $6n+1$.

Todistus. (Vrt. apulause 3.14.) Todistuksessa riittää jälleen tarkastella kahden kokonaisluvun tuloa. Olkoon nyt $l = 6k+1$ ja $l' = 6t+1$. Kertomalla nämä luvut yhteen saadaan

$$ll' = (6k+1)(6t+1) = 36kt + 6k + 6t + 1 = 6(6kt + k + t) + 1.$$

Tämä on muotoa $6n+1$, joten kahden muotoa $6n+1$ olevan kokonaisluvun tulo on edelleen muotoa $6n+1$. □

Esimerkki 3.18. Olkoon $n_1 = 3$ ja $n_2 = 4$. Nyt

$$\begin{aligned}(6n_1+1)(6n_2+1) &= (6\cdot 3+1)(6\cdot 4+1) = (18+1)(24+1)\\ &= 19\cdot 25 = 475 = 474+1 = 6\cdot 79+1,\end{aligned}$$

joka on muotoa $6n+1$.

Lause 3.19. *On olemassa ääretön määrä muotoa* $6n+5$ *olevia alkulukuja. [1, s. 58]*

Todistus. Tehdään nyt vastaoletus, että on olemassa äärellinen määrä muotoa $6n+5$ olevia alkulukuja siten, että

$$p_0 = 5 < p_1 < p_2 < \cdots < p_n.$$

Huomioidaan, että kokonaisluku

$$N = 6p_1p_2\cdots p_n + 5$$

ei ole jaollinen luvulla 2, kun $N > 1$. Apulauseen 3.17 perusteella kokonaisluvulla N on ainakin yksi alkulukutekijä p, joka on muotoa $6k+5$. Jos $p = 5$, niin

$$5 \mid N - 5 = 6p_1p_2\cdots p_n.$$

Nyt koska $5 = p_0$, niin 5 ei ole mikään tulossa $6p_1p_2\cdots p_n$ esiintyvistä alkuluvuista. Tällöin tulo ei voi olla jaollinen luvulla 5, joten kyseessä on ristiriita. Toisaalta jos $p > 5$, niin

$$p \mid N - 6p_1p_2\cdots p_n = 5.$$

Tämä on ristiriita, koska $p > 5$, joten se ei voi jakaa lukua 5. Molemmissa tapauksissa on siis kyseessä ristiriita, joten muotoa $6n+5$ olevia alkulukuja on olemassa ääretön määrä. □

3.5 Muotoa $8n+3$ olevat alkuluvut

Esitetään vielä kolmas tapa todistaa tiettyä muotoa olevien alkulukujen äärettömyys. Lauseessa 3.30 todistetaan muotoa $8n+3$ olevien alkulukujen äärettömyys.

Esitetään ensin neliönjäännöksen ja Legendren symbolin määritelmät sekä apulauseet 3.24 ja 3.26, joita tarvitaan todistuksen ymmärtämiseen.

Määritelmä 3.20. (Vrt. [2, s. 44].) Olkoon m positiivinen kokonaisluku ja a sellainen kokonaisluku, että $\operatorname{syt}(a, m) = 1$. Nyt a on *neliönjäännös* $\pmod m$, jos kongruenssi $x^2 \equiv a \pmod m$ on ratkeava. Muutoin kyseessä on *neliönepäjäännös*.

Esimerkki 3.21. Olkoon $m = 7$. Nyt neliönjäännöksien selvittämiseksi täytyy tietää, millä arvoilla $a = 1, 2, \ldots, 6$ kongruenssi $x^2 \equiv a \pmod 7$ on ratkeava. Tällöin määritelmän 3.20 mukaan luvut 1, 2 ja 4 ovat neliönjäännöksiä $\pmod 7$, sillä

$$6^2 \equiv 1 \pmod 7, \qquad 4^2 \equiv 2 \pmod 7 \qquad \text{ja} \qquad 5^2 \equiv 4 \pmod 7.$$

Vastaavasti luvut 3 ja 6 ovat neliönepäjäännöksiä $\pmod 7$.

Määritelmä 3.22. (Vrt. [2, s. 46].) Olkoon p pariton alkuluku ja $\text{syt}(a, p) = 1$. Tällöin *Legendren symboli* $\left(\frac{a}{p}\right)$ määritellään siten, että

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{jos } a \text{ on neliönjäännös } \pmod p, \\ -1, & \text{jos } a \text{ on neliönepäjäännös } \pmod p. \end{cases}$$

Esimerkki 3.23. Nyt esimerkin 3.21 mukaan 2 on neliönjäännös $\pmod 7$ ja 3 on neliönepäjäännös $\pmod 7$. Tällöin määritelmän 3.22 perusteella

$$\left(\frac{2}{7}\right) = 1 \qquad \text{ja} \qquad \left(\frac{3}{7}\right) = -1.$$

Seuraavaa apulausetta kutsutaan *resiprookkilaiksi*.

Apulause 3.24. Jos p ja q ovat erisuuria, parittomia alkulukuja, niin

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{q-1}{2}\right)\left(\frac{p-1}{2}\right)}.$$

Todistus. Ks. [2, s. 47]. □

Esimerkki 3.25. Olkoon $p = 5$ ja $q = 7$. Nyt resiprookkilain 3.24 perusteella saadaan

$$\left(\frac{5}{7}\right)\left(\frac{7}{5}\right) = (-1)^{\left(\frac{7-1}{2}\right)\left(\frac{5-1}{2}\right)} = (-1)^{3\cdot 2} = 1.$$

Apulause 3.26. Jos p on pariton alkuluku, niin $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Todistus. Ks. [2, s. 50]. □

Esimerkki 3.27. Olkoon $p = 5$. Nyt apulauseen 3.26 perusteella saadaan

$$\left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = (-1)^3 = 1.$$

Näitä ominaisuuksia hyödynnetään seuraavan apulauseen 3.28 todistamisessa.

Apulause 3.28. Jos $p \mid (x^2 + 2)$, niin joko $p \equiv 1 \pmod 8$ tai $p \equiv 3 \pmod 8$. [2, s. 79]

Todistus. Olkoon $p \geq 3$ alkuluku. Oletetaan, että on olemassa positiivinen kokonaisluku x siten, että $p \mid (x^2 + 2)$. Nyt $x^2 \equiv -2 \pmod{p}$, jolloin määritelmän 3.20 perusteella -2 on neliönjäännös $\pmod{p}$. Nyt koska $-2 = (-1) \cdot 2$, niin voidaan määritelmän 3.22 ja apulauseiden 3.24 ja 3.26 perusteella kirjoittaa

$$\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}} = 1.$$

Nyt jos $p \mid (x^2 + 2)$, niin kongruenssi $\frac{p-1}{2} \equiv \frac{p^2-1}{8} \pmod{2}$ pätee. Jäännösluokkia tarkastelemalla voidaan todeta, että kongruenssi pätee silloin, kun $p \equiv 1 \pmod{8}$ tai $p \equiv 3 \pmod{8}$. □

Apulause 3.29. Kahden tai useamman muotoa $8n + 1$ olevan kokonaisluvun tulo on edelleen muotoa $8n + 1$.

Todistus. (Vrt. apulause 3.14.) Todistuksessa riittää jälleen tarkastella kahden kokonaisluvun tuloa. Olkoon nyt $l = 8k + 1$ ja $l' = 8t + 1$. Kertomalla nämä luvut yhteen saadaan

$$ll' = (8k + 1)(8t + 1) = 64kt + 8k + 8t + 1 = 8(8kt + k + t) + 1,$$

joka on muotoa $8n + 1$. □

Näiden tietojen avulla voidaan esittää todistus siitä, että muotoa $8n + 3$ olevia alkulukuja on ääretön määrä.

Lause 3.30. *On olemassa ääretön määrä muotoa* $8n + 3$ *olevia alkulukuja. [2, s. 79]*

Todistus. Tehdään vastaoletus, että on olemassa äärellinen määrä muotoa $8n+3$ olevia alkulukuja, joita merkitään symboleilla $q_1, \ldots, q_k$. Tarkastellaan kokonaislukua

$$N = (q_1 \cdots q_k)^2 + 2, \qquad \text{missä } N > 1.$$

Apulauseen 3.28 perusteella tiedetään, että jokainen luvun N alkulukutekijä on joko muotoa $q = 8k + 1$ tai $q = 8k + 3$. Jos kaikki alkulukutekijät ovat muotoa $8k + 1$, niin apulauseen 3.29 perusteella niiden tulo on myös muotoa $8k + 1$. Tämä ei kuitenkaan ole mahdollista, koska $N \equiv 3 \pmod{8}$. Tämä tarkoittaa, että on olemassa alkuluku $q = 8k + 3$, jolla N on jaollinen. Nyt q ei kuitenkaan voi olla mikään q_i, koska $\text{syt}(q_i, N) = \text{syt}(q_i, 2) = 1$. Tämä on ristiriita, joten muotoa $8n + 3$ olevia alkulukuja on ääretön määrä. □

Lähteet

[1] D. M. Burton. *Elementary number theory*, 6th ed. New York: McGraw-Hill, 2007. ISBN-13 978-0-07-305I88-8.

[2] B. Fine, & G. Rosenberger. *Number theory: An introduction via the distribution of primes*. Boston: Birkhäuser, 2007. ISBN-13 978-0-8176-4472-7.

[3] K. H. Rosen. *Elementary number theory and its applications*, 6th ed. Boston: Pearson, 2011. ISBN-13: 978-0-321-50031-1.